IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor:	Pradeep Bahl	Attorney Docket No.:	147649.01
Application No.:	09/607,195	Group Art Unit	2135
Filed:	06/28/2000	Examiner:	Dada, Beemnet
Customer No.:	22971	Confirmation Number:	7584
Title: METHOD FOR CONTROLLING ACCESS TO A NETWORK BY A WIRELESS CLIENT			

APPEAL BRIEF

To: Commissioner for Patents
PO Box 1450
Alexandria, Virginia 22313-1450

From: Microsoft Corporation,
Customer No. 22971

Pursuant to 37 C.F.R. §41.37, Applicant hereby submits an appeal brief for application 09/607,195, filed June 28, 2000, within the requisite time from the date of filing the Notice of Appeal. Accordingly, Applicant appeals to the Board of Patent Appeals and Interferences seeking review of the Examiner's rejections.

Real Party in Interest

The real party in interest is Microsoft Corporation, the assignee of all right, title and interest in and to the subject invention.

Related Appeals and Interferences

Appellant is not aware of any other appeals, interferences, or judicial proceedings which will directly affect, be directly affected by, or otherwise have a bearing on the Board's decision to this pending appeal.

Status of Claims

Claims 1-33 stand rejected and are pending in the Application. Claims 1-33 are appealed. Claims 1, 9, 12-14, 16, 24, and 31-33 were previously amended. Claims 1-33 are set forth in the Appendix of Appealed Claims on page 23.

Status of Amendments

An Office Action was issued on February 3, 2004.

A response to the Office Action was filed on June 3, 2004. Claims 1, 9, 12 -14, 16, and 24 were amended. Claims 31-33 were added.

An Office Action was issued on December 21, 2004.

A response to the Office Action was filed on February 17, 2005. No claims were amended.

A Final Office Action was issued on July 8, 2005.

A response to the Office Action was filed on September 8, 2005. No claims were amended.

An Advisory Action was issued on October 7, 2005.

An Amendment After Final Office Action was filed on December 7, 2005. Claims 1 and 12 were amended.

A Request for Continued Examination was filed on January 13, 2006.

An Office Action was issued on March 22, 2006.

A response to the Office Action was filed June 22, 2006. No claims were amended.

A Final Office Action was issued on September 6, 2006.

A response to the Final Office Action was filed November 6, 2006. No claims were amended.

An Advisory Action was issued on November 27, 2006, indicating that the request for reconsideration had been considered but did not place the application in condition for allowance.

Appellant filed a Notice of Appeal on December 14, 2006 in response to the Final Office Action.

Summary of Claimed Subject Matter

The pending independent claims are claims 1, 9, 12, and 21. A concise explanation of each of the independent claims is provided below.

Claim 1 is directed to a method for controlling access to a network by a wireless client (FIG. 4 and FIG. 5, page 10 line 8 – page 13, line 22). The

method comprises assigning a network address including a lease period to the wireless client (316 in FIG. 5, page 11, lines 6-11), sending the assigned network address to the wireless client prior to establishing a secure link (318 in FIG. 5, page 11, lines 11-15), establishing the secure link using the assigned network address (326 in FIG. 5, page 12, lines 8-14), and sending an address of a wireless access point to the wireless client (330 in FIG. 5, page 13, lines 2-7).

Claim 9 is directed to a method for controlling access to a network by a wireless client using an assigned network address including a lease period (FIG. 4 and FIG. 5, page 10 line 8 - page 13, line 22). The method comprises engaging in a negotiation of a secure link with the wireless client (330 in FIG. 5, page 13, lines 2-7), communicating with an address server of the network to determine whether the lease period of the leased network address has expired (332 in FIG. 5, page 13, lines 13-15), and if the lease period is determined to be expired, terminating the negotiation (page 13, lines 14-16).

Claim 12 is directed to a method for controlling access to a network by a wireless client (FIG. 4 and FIG. 5, page 10 line 8 - page 13, line 22). The method comprises receiving a request for a network address from the wireless client (312 in FIG. 4, page 10, line 23 - page 11, line 2), attaching information to the request to indicate that the request originated from a wireless client and relaying the request to the address server (314 in FIG. 4, page 11, lines 3-5), receiving an assignment of an address having a lease time from the address server (316 in FIG. 5, page 11, lines 6-11), relaying the assignment of the address to the wireless client (318 in FIG. 5, page 11, lines 11-15), and

negotiating the establishment of a secure link with the wireless client using the assigned address (330 in FIG. 5, page 13, lines 2-7).

Claim 21 is directed to a method for gaining access to a network by a wireless client. The method comprises broadcasting a request for an address on the network (310 in FIG. 4, page 10, lines 21-23), receiving an assignment of a leased address including a lease time from the network (316 in FIG. 5, page 11, lines 6-11), and negotiating a secure link with the network before the lease time expires (320, 322, 324 in FIG. 5, page 11, line 16 - page 12, line 7).

Grounds of Rejection to be Reviewed on Appeal

Independent Claim 12 stands rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6.704,789 to Ala-Laurila (hereinafter "Ala-Laurila"). Claims 13-16, 19, and 20 depend from Claim 12. Claims 15 and 19 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Ala-Laurila. Claims 13, 14, 16, and 20 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Ala-Laurila in view of U.S. Patent 6, 510, 153 to Inoue et al. (hereinafter "Inoue").

Independent Claims 9 and 21 stand rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,884,024 to Lim et al. (hereinafter "Lim"). Claims 10, 11, and 17 depend from Claim 9. Claims 22-30 depend from Claim 21. Claims 11 and 17 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Lim. Claim 10 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Lim in view of Ala-Laurila. Claims 22, 24-27, 29, and 30 stand rejected under 35 U.S.C. 102(b) as being anticipated by Lim. Claim 23

and 28 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Lim in view of Ala-Laurila.

Independent Claim 1 stands rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent 6,061, 346 to Nordman in view of US 20020023160 A1 to Garrett et al. (hereinafter Garrett). Claims 2-8 and 31-33 depend from Claim 1. Claims 2-8 and 31-33 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Nordman in view of Garrett.

Argument

I. The rejection under 35 U.S.C. §102(e) over Ala-Laurila is improper because Ala-Laurila does not anticipate each and every element of the claims.

Claims 12, 15, and 19 stand rejected under 35 U.S.C. §102(e) as being anticipated by Ala-Laurila.

The Applicant respectfully submits that the Office has not established a proper anticipation rejection because Ala-Laurila does not anticipate each and every element of the claims.

A. The §102 Standard

In making out a §102 rejection, the Federal Circuit has stated that "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegall Bros. v. Union Oil Co. of California*, 814, F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Furthermore, "[t]he identical invention must be

shown in as complete detail as is contained in the...claim...." *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990).

B. Summary of Disclosure in Ala-Laurila

In general, Ala-Laurila discloses using a subscriber identification module (SIM) to authenticate a user to a first network using authentication information stored at a second network. A "SIM" is a smartcard typically used in a mobile telephone to store information used to identify and authenticate subscribers on a mobile phone carrier's mobile phone network. Ala-Laurila generally discloses a method in which the identification of a user is transmitted to a second network and authentication information of the user stored in the second network is calculated using the user's SIM card, then transmitted from the second network to a first network, allowing the user access to the first network.

C. Summary of Key Differences Between Application and Ala-Laurila

Ala-Laurila is similar to the application only in that Ala-Laurila uses the Dynamic Host Resolution Protocol (DHCP) to assign an Internet Protocol (IP) address to a user's device. To wit, Ala-Laurila is primarily directed to user authentication using a mobile phone SIM card.

In contrast, the application discloses a method for a wireless device to obtain a short-lease IP address from a wireless access point connected to a network, then establishing a secure link using the short-leased IP address, and finally renewing the lease for a longer duration using the secure link. If the user

is unable to establish the secure link, the short-leased IP address expires and the user no longer has access to the network.

In particular, while both Ala-Laurila and the present application are directed to either granting or denying access to a network, the method by which access is granted or denied differs vastly.

D. Claim 12

Claim 12 is directed to a method for controlling access to a network by a wireless client. The method comprises (1) receiving a request for a network address from the wireless client, (2) attaching information to the request to indicate that the request originated from a wireless client and relaying the request to the address server, (3) receiving an assignment of an address having a lease time from the address server, (4) relaying the assignment of the address to the wireless client, and (5) negotiating the establishment of a secure link with the wireless client using the assigned address.

The Office asserts that asserts that Ala-Laurila discloses receiving a request for a network address from the wireless client as "steps DHCP SOLICIT, figures 4 & 5" (*see* page 5, Final Office Action of 09/06/2006, point 11) . Consider that the DHCP SOLICIT message is included as part of the Dynamic Host Configuration Protocol, and is a message sent by a client to receive the address of one or more DHCP servers. The DHCP SOLICIT message is not sent to request a network address.

In particular, a network address may not be requested from a DHCP server until the address of one or more DHCP servers is located by a client.

More particularly, logic dictates that a client may not request a network address from a DHCP server if the client does not have the address of a DHCP server to which the request may be sent.

To that end, Ala-Laurila includes "Dynamic Host Configuration Protocol For IPv6 (DHCPv6) Work in Progress DHCP Working Group 1998, J. Bound and C. Perkins" by reference (see Ala-Laurila, col. 3, lines 27-29; hereafter "Bound and Perkins"). Note that Bound and Perkins disclose the DHCPv6 command DHCP SOLICIT as sent by a client to locate a DHCPv6 server. For example, see Bound and Perkins, Section 5.2 "Sending DHCP Solicit Messages", "[t]he client MUST have the address of a server to sent a request message" and "[t]he client SHOULD locate a DHCP server by multicasting a DHCP Solicit message to the All-DHCP-Agents link-local multicast address".

The Office may assert that sending the DHCP SOLICIT command may be broadly interpreted as a request for a network address. However, such a broad interpretation is not appropriate. The DHCP SOLICIT message instructs the DHCP server to perform a specific operation. For example, even if a client sends the DHCP SOLICIT command to discover the network address of one or more DHCP servers, the client is not required or obligated to send the DHCP REQUEST message to request a network address.

Rather, the Office has purposely chosen to create an equivalency between the DHCP SOLICIT message and a "request for a network address" such that the Office may further assert that "attaching information to the request to indicate that the request originated from a wireless client" is disclosed at Figures 4 and 5 of Ala-Laurila as "USER ID attached to the DHCP SOLICIT" (*see* Final Office Action

of 09/06/2006, page 5, point 11). However, as it has already been established that the DHCP SOLICIT message is not a request for a network address, it logically follows that any information attached to the DHCP SOLICIT message is not information attached to a request for a network address.

The Office continues the rejection by asserting that the USER ID of Ala-Laurila is equivalent to "information..to indicate that the request originated from a wireless client" (*see* Final Office Action of 09/06/2006, page 5, point 11). However, Ala-Laurila does not disclose that the USER ID includes any such information. In contrast, Ala-Laurila discloses the USER ID at col. 5, lines 56-61 as follows:

"The smart card associated with the user terminal 12, which may be of diverse designs, provides the user identification (USER ID) as described below in conjunction with FIGS. 4-6 and may be without limitation IMSI or NAI (Network Access Identifier) in accordance with RFC 2486."

As disclosed by Ala-Laurila, a Network Access Identifier is defined in RFC 2486 (hereinafter "RFC 2486") at Section 2.4, "Notes for Implementors":

"[a]s proposed in this document, the Network Access Identifier is of the form user@realm".

Ala-Laurila's disclosure of the USER ID is consistent with that of RFC 2486 in that Ala-Laurila discloses that the USER ID is used to authenticate the user of a device. And, as expected, Ala-Laurila is silent with regard to the USER ID being used or usable as "information..to indicate that the request originated from a wireless client." That is, "information...to indicate that the request originated from a wireless client" is not used by Ala-Laurila, as Ala-Laurila is

primarily directed to authenticating users of wireless devices - for example, mobile phones including a SIM card - and such information would be redundant.

The Office continues the rejection, asserting that "relaying the request to the address server" is disclosed in Ala-Laurila at "figure 4, 5, units 24 & 14" (*see* Final Office Action of 09/06/2006, page 5, point 11) . Ala-Laurila does disclose the RELAY 24 of FIG. 4 as forwarding a DHCP SOLICIT message to the SERVER 14 of FIG. 4. However, the DHCP SOLICIT message of Ala-Laurila is not a "request for a network address", as has already been established. The "USER ID" of Ala-Laurila is not "information...to indicate that the request originated from a wireless client", as has already been established. Therefore, the RELAY 24 of FIG. 4 is not "relaying the request [for a network address]" to the SERVER 14 of FIG. 4 and the RELAY 24 of FIG. 4 is not "relaying the request including information...to indicate that the request originated from a wireless client".

However, if the Office is asserting that the DHCP REQUEST message of FIG. 4 of Ala-Laurila is a "request for a network address", the Office has already attempted to draw an equivalency between the DHCP SOLICIT + USER ID message of FIG. 4 as a "request for a network address". Furthermore, the Office has also failed to establish that the DHCP REQUEST message of FIG. 4 of Ala-Laurila has "attached information...to indicate that the request originated from a wireless client". To wit, the DHCP REQUEST message of FIG. 4 of Ala-Laurila is not shown or disclosed as including information to indicate that the request originated from a wireless client.

For at least the above-identified reasons, the Applicant respectfully submits that **Claim 12** is not anticipated by Ala-Laurila and is allowable. Accordingly, the rejection of **Claim 12** should be withdrawn.

E. Claims 13-16 and 19-20

Claims 13-16 and 19-20 depend from **Claim 12** and are allowable at least by virtue of that dependency. Accordingly, the rejection of **Claims 13-16 and 19-20** should be withdrawn.

II. The rejection under 35 U.S.C. §102(b) over Lim is improper because Lim does not anticipate each and every element of the claims.

Claims 9, 11, 17, 21, 22, 24-27, 29 and 30 stand rejected under 35 U.S.C. §102(b) as being anticipated by Lim.

The Applicant respectfully submits that the Office has not established a proper anticipation rejection because Lim does not anticipate each and every element of the claims.

A. The §102 Standard

In making out a §102 rejection, the Federal Circuit has stated that "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegall Bros. v. Union Oil Co. of California*, 814, F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Furthermore, "[t]he identical invention must be shown in as complete detail as is contained in the...claim...." *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990).

B. Summary of Disclosure in Lim

Lim is generally directed to "a preferred method for renewal of an IP address lease by DHCP server system" and not to engaging in a negotiation of a secure link with the wireless client as in **Claims 9 and 21**. Furthermore, Lim is generally directed to extending the DHCP protocol to allow a server to check a database to determine whether the requestor of an address should be assigned an address. The DHCP server system of Lim is not configured to manage links; rather, the DHCP server system of Lim is configured to, inter alia, assign internet protocol (IP) addresses to trusted clients and manage lease times and renewals for trusted clients.

C. Claims 9 and 21

Claim 9 is directed to a method for controlling access to a network by a wireless client using an assigned network address including a lease period. The method comprises engaging in a negotiation of a secure link with the wireless client, communicating with an address server of the network to determine whether the lease period of the leased network address has expired, and if the lease period is determined to be expired, terminating the negotiation (page 13, lines 14-16).

Claim 21 is directed to a method for gaining access to a network by a wireless client. The method comprises broadcasting a request for an address on the network, receiving an assignment of a leased address including a lease time

from the network, and negotiating a secure link with the network before the lease time expires.

In rejecting **Claim 9**, the Office asserts that Lim discloses engaging in a negotiation of a secure link with the wireless client at column 7, lines 21-30 (*see* page 6, Final Office Action of September 9, 2006, point 13). Lim discloses the following at Column 7, lines 21-30:

"A preferred method for renewal of an IP address lease by DHCP server system **110** is shown in FIG. **7** and generally designated **700**. Method **700** begins with step **702** where DHCP server system **110** receives a broadcast DHCPREQUEST message from a client system **102**. For the purposes of illustration, it is assumed that the DHCPREQUEST message does not identify a specific DHCP server **110**. Thus, according to the DHCP protocol, the received message is a request from a client system **102** for renewal of an existing lease."

The cited section of Lim does not disclose any type of secure link, a wireless client, or the engaging in a negotiation of a secure link with a wireless client. Rather, the above cited section of Lim is directed to "a preferred method for renewal of an IP address lease by [the] DHCP server system". The renewal of an IP address lease cannot be considered equivalent to engaging in a negotiation of a secure link with a wireless client regardless of how broadly the cited section is interpreted by the Office.

In particular, the cited section of Lim is discloses a DHCP server system. A DHCP server responds to DHCP messages sent by a client that is requesting an IP address from the DHCP server. A DHCP server does not engage in negotiation of secure links or any other type of link. More particularly, the DHCP server

system disclosed by Lim extends the DHCP protocol such that the DHCP server system of Lim is only configured to, *inter alia*, assign internet protocol (IP) addresses to trusted clients and manage lease times and renewals for trusted clients.

The Office continues the rejection, asserting that "communicating with an address server of the network to determine whether the lease period of the leased network address has expired" and "if the lease period is determined to be expired, terminating the negotiation, thereby preventing the wireless client from accessing the network" is disclosed at column 8, lines 33-55 of Lim (*see* page 6, Final Office Action of September 9, 2006, point 13).

Lim discloses the following at column 8, lines 33-55:

"If the terms of the lease continuation are acceptable to the DHCP server system **110**, method **700** continues at step **720**. In step **720**, the DHCP server system **110** determines if the lease included in the retrieved record **500** has expired. If not method **700** continues at step **722** where the DHCP server system **110** updates the lease database **316** to indicate that the lease included in the retrieved record **500** has been renewed by the client system **102**. Step **722** is followed by step **724** where the DHCP server system **110** sends the client system **102** a DHCPACK message. The DCHPACK message informs the client system **102** that the IP address lease has been renewed.

If the DHCP server system **110** determines, in step **720**, that the lease included in the retrieved record **500** has expired, method **700** continues at step **726**. In step **726**, the DHCP server system **110** uses the trusted identifier extracted in step **704** to search the trusted identifier database **318**. More

specifically, the DHCP server system **110** uses the retrieved trusted identifier to search the trusted identifier index **602** of the trusted identifier database **318**. If an entry is found in the trusted identifier index **602** that matches the retrieved trusted identifier, the DHCP server system **110** retrieves the corresponding record."

Even given its broadest possible interpretation, the section of Lim cited by the Office fails to disclose the elements of **Claim 9**. In particular, the cited section of Lim fails to disclose a wireless client and a secure link being negotiated with the wireless client. Therefore, because the cited section of Lim fails to disclose these elements, the cited section of Lim is further not able to disclose terminating the negotiation of the secure link with the wireless client if the lease period is determined to be expired. The cited section of Lim also fails to disclose that the termination of the negotiation of the secure link with the wireless client has the effect of preventing access to the network by the wireless client.

Rather, the cited section of Lim discloses, in general, that the DHCP server system includes a database of trusted identifiers associated with clients. Lim further discloses that the DHCP server system examines the database and associated indices to determine if the trusted identifier is included in the database, and if so, renews the lease granted to the client associated with the trusted identifier.

However, the Office asserts that a secure link is inherent in the DHCP server system of Lim, stating, "Examiner would point out that, Lim teaches a trusted identifier, that can not be forged by a client system (i.e., secure system)

for engaging in negotiation of a secure link with a wireless client (i.e., a secure link) [see column 7, lines 6-56]" (*see* Final Office Action of September 6, 2006, Page 3, point 6). First, consider that a DHCP server is not configured to manage links; rather, a DHCP system is directed to assign IP addresses to clients. Next, consider that a trusted identifier does not need to be transferred between client and server over a "secure link"; a trusted identifier may be encrypted, digitally signed, or employ some other form of secrecy such that the trusted identifier may be passed in plain text over a non-secure link and still remain a trusted identifier as is known to one of ordinary skill in the art.

Finally, while the section of Lim cited by the Office does disclose IPSEC authentication, Lim discloses use of the IPSEC authentication header, which is not equivalent to a secure link. As is known to one of skill in the art, the IPSEC authentication header establishes a security association between two devices; a security association is not equivalent to a secure link. For example, consider that the link between the two devices sharing a security association may still be insecure; there is no requirement that the link between the two devices sharing a security association be secure. For these reasons, the Office's assertion that negotiation of secure links is inherent in the cited section of Lim is incorrect.

With regard to **Claim 21**, the Office asserts that "negotiating a secure link with the network before the time lease expires" is also disclosed at column 8, lines 33-55 of Lim (*see* page 6, Final Office Action of September 9, 2006, point 13). As discussed above with regard to **Claim 9**, the cited section of Lim fails to inherently or expressly disclose the negotiation of a secure link.

For at least the above-identified reasons, **Claims 9 and 21** are not anticipated by Lim and are allowable. Accordingly, the rejection of **Claims 9 and 21** should be withdrawn.

D. Claims 10-11, 17-18, and 22-30

Claims 10-11 and 17-18 depend from **Claim 9** and are allowable at least by virtue of that dependency. Accordingly, the rejections of **Claim 10-11 and 17-18** should be withdrawn. **Claims 22-30** depend from **Claim 21** and are allowable at least by virtue of that dependency. Accordingly, the rejections of **Claims 22-30** should be withdrawn.

III. The rejection under 35 U.S.C. §103(a) over the combination of Nordman and Garrett does not establish a *prima facie* case of obviousness.

Claims 1-8 and 31-33 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent 6,061,346 to Nordman (hereinafter "Nordman") in view of U.S. Patent Application 20020023160 A1 to Garrett et al. (hereinafter "Garrett").

Applicant respectfully submits that the Office has not established a *prima facie* case of obviousness with respect to establishing that the prior art teaches or suggests all elements of the claims.

A. The §103 Standard

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary

skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

B. Summary of Disclosure in Nordman and in Garrett

Nordman is generally directed to a method for allowing a network-located device to access a second private network by authenticating the network-located device using various methods. Garrett is generally directed to a method for managing the forwarding of network packets between networks managed by different service providers.

C. Claim 1

The Office asserts that Nordman teaches the method as recited in **Claim 1** (*see* page 8, Final Office Action issued on September 9, 2006, point 20) with the exception being that "Nordman is silent on sending the assigned network address to the wireless client prior to establishing a secure link". The Office goes on to assert that the deficiency of Nordman is solved by the combination of Garrett, stating, "within the same field of endeavor Garrett teaches assigning a network address, sending the assigned network address to the client prior to establishing a secure link and establishing a secure link using the assigned

network address (figure 9, steps 902-907, note that authentication at steps 904-906 is performed after the address is assigned and provided to the client at steps 902 & 903)."

The Office asserts that the motivation to combine the disclosure of Nordman with the disclosure of Garrett is to "allow authorized use of IP address and further enhance the security of the system". However, consider that Nordman already includes "security of the system" (*see* Nordman's title, "Secure Access Method, and Associated Apparatus, For Accessing a Private IP Network").

In addition, both Nordman and Garrett "allow authorized use of IP address" so there is no need for Nordman to be combined with Garrett to allow such functionality. For example, see Nordman, column 4, lines 17-19 "[a]n IP address is allocated to the wireless host by the private IP network", and see Garrett, page 1, paragraph [0006], "a configuration server, upon receiving a request from a network access device selecting a particular service, allocates a network address from a pool of addresses associated with the service and assigns the network address to the network access device using a host configuration protocol, such as DHCP."

Therefore, the Office has failed to establish a suggestion or motivation, either in the Nordman or Garrett, to modify Nordman with the teachings of Garrett or to combine Nordman and Garrett. To the contrary, the Office's stated motivation to combine is instead a motivation not to modify Nordman with the teachings of Garrett.

The Office has also failed to establish that there is a reasonable expectation of success in combining Nordman with the teachings of Garrett.

The Office cites FIG. 9, and the steps performed by the "RADIUS Server 930" as solving the deficiency in address allocation of Nordman recited at column 4, lines 13-22 (*see* page 8, Final Office Action issued on September 9, 2006, point 20). However, one of ordinary skill in the art will arrive at the conclusion that the RADIUS Server 930 of Garrett may not be successfully combined with the system of address allocation in Nordman. To wit, the "RADIUS Server 930" from FIG. 9 of Garrett is defined in Garrett at paragraph 36 as follows:

"Alternatively, the DHCP server 161 in the service activation system 160 can interact with the registration server 155 using a back-end authentication protocol, e.g. the Remote An Authentication Dial In User Service (RADIUS). See C. Rigney, A. Rubens, W. Simpson, S. Willens, "Remote Authentication Dial In User Service (RADIUS)," IETF Network Working Group, RFC 2058 (January 1997), which is incorporated by reference herein. The DHCP server can contain a RADIUS client and, thereby, leverage the large RADIUS embedded base used for dial access authentication.

...

The DHCP server 920 forwards both the challenge and response in a RADIUS_ACCESS_REQ message to a RADIUS server 930 in the selected service network. The RADIUS server 930 either accepts or rejects the RADIUS request and responds accordingly at 906. If the RADIUS request is accepted, the DHCP server 920 sends a DHCPACK message at 907 and the client 910 enters a bound state. If the RADIUS request is rejected, the DHCP server 920 sends a DHCPNACK message which informs the client 910 that the IP address that was allocated has been withdrawn."

The RADIUS Server 930 of Garrett is defined as server providing remote authentication dial in user service. The address allocation system of Nordman provides addresses to wireless clients. The RADIUS Server 930 may not be used by a client of Nordman, as the client of Nordman does not "dial in" to request a network address. Rather, the client of Nordman is wireless and requests a network address via a wireless connection. Therefore, the RADIUS Server 930 of Garrett will not be successful in communicating with the clients or servers of Nordman.

Finally, neither Nordman or Garrett, either alone or in combination, teach or suggest all the limitations of **Claim 1**. For example, the Office asserts that Nordman teaches "the wireless access point is adapted to handle the secure link established by the wireless client" at column 8, lines 12-23 and lines 57-67 (*see* page 8, Final Office Action issued on September 9, 2006, point 20). Nordman recites the following at column 8, lines 12-23:

"WHI, and other data, between the private IP network 14 and the wireless access network formed of the network infrastructure. Such authenticated tunneling is performed as the backbone network 46 might be shared by many different operators and security of the backbone can not be assured. For instance, if the HIPN 106 is to be accessed, data is routed by way of a public Internet 108. The authenticated IP tunneling is performed to authenticate traffic, i.e., communication of data, between the SGSN 82 and the GGSN 92. Authenticating the traffic routed over the backbone ensures the validity of the value of the WHI when the value is received at the GGSN 92. When, e.g., the HIPN 102 is instead to be accessed, the transmission over the Internet 104"

And Nordman recites the following at column 8, lines 547-67:

"During the attach procedure, the values of the IMSI, the WHI, and other associated subscriber data is downloaded from the HLR 76 to the appropriate one of the MSC/VLR 66 and SGSN 82. The other appropriate subscriber data includes the address of the private IP network 14. Addresses of additional private IP networks, such as the HIPN 96, 102, and 106 (shown in FIG. 1) may also be downloaded to permit alternate, or second-choice access to an alternate IP network. The HIPN address identifying the private IP network 14, in one embodiment, is the address of the GGSN, such as the GGSN 92 of the private IP network 14."

Nordman recites that "the private IP network 14 and the wireless access network formed of the network infrastructure" are adapted to handle a secure link. Nordman does not recite that a wireless access point is adapted to handle a secure link. Even if Nordman were to recite a wireless access point adapted to handle a secure link, Nordman is silent with regard to the secure link being established by a wireless client as in **Claim 1.**

Therefore, the Office has failed to establish a *prima facie* case of obviousness using any of the three basic criteria. Therefore, **Claim 1** is allowable and the rejection to **Claim 1** should be removed.

D. Claims 2-8 and 31-33

Claims 2-8 and 31-33 depend from **Claim 1** and are allowable at least by virtue of that dependency.

Conclusion

The Office's basis and supporting rationale for the § 102(e), 102(b) and 103(a) rejections is not supported by the disclosure of the cited references. Applicant respectfully requests that the rejections be overturned and that the pending claims be allowed to issue.

Respectfully Submitted,

Dated: June 4, 2007 By: /Stephen Siu/

Stephen Siu, Reg. No. 48,303
Attorney for Applicants
Direct telephone (425) 704-0669
Microsoft Corp.
One Microsoft Way,
Redmond, WA 98052
Drafted by Peter Taylor

CERTIFICATE OF MAILING OR TRANSMISSION [37 CFR 1.8(a)]

I hereby certify that this correspondence and the documents identified on this form are being electronically deposited with the USPTO via EFS-Web on the date shown below:

June 4, 2007 /Kate Marochkina/

Date Kate Marochkina

Appendix of Appealed Claims

1. (Previously Presented) A method for controlling access to a network by a wireless client, the method comprising:

assigning a network address to the wireless client, wherein the network address has a lease period;

sending the assigned network address to the wireless client prior to establishing a secure link;

establishing the secure link using the assigned network address; and

sending an address of a wireless access point to the wireless client, wherein the wireless access point is adapted to handle the secure link established by the wireless client.

2. (Original) The method of claim 1, wherein the assigned network address and the wireless access point address are sent to the wireless client in a DHCP offer packet.

3. (Original) The method of claim 1, wherein the secure link is an IPSEC tunnel.

4. (Original) The method of claim 1, wherein the assigned network address is sent to the wireless client via the wireless access point.

5. (Original) The method of claim 1, wherein the address of the wireless access point that is sent to the wireless client comprises an IP address and a MAC address.

6. (Original) A computer-readable medium having stored thereon computer-executable instructions for performing the method of claim 1.

7. (Original) A computer-readable medium having stored thereon computer-executable instructions for performing the method of claim 2.

8. (Original) A computer-readable medium having stored thereon computer-executable instructions for performing the method of claim 3.

9. (Previously Presented) A method for controlling access to a network by a wireless client, the wireless client using an assigned network address having a lease period to communicate with the network, the method comprising:

engaging in a negotiation of a secure link with the wireless client;

communicating with an address server of the network to determine whether the lease period of the leased network address has expired; and

if the lease period is determined to be expired, terminating the negotiation, thereby preventing the wireless client from accessing the network.

10. (Original) The method of claim 9, wherein the negotiation is a negotiation of an IPSEC tunnel.

11. (Original) The method of claim 9, wherein the address server is a DHCP server.

12. (Previously Presented) A method for controlling access to a network by a wireless client, the method comprising:

receiving a request for a network address from the wireless client;

attaching information to the request to indicate that the request originated from a wireless client;

relaying the request to the address server;

receiving an assignment of an address from the address server, the address having a lease time;

relaying the assignment of the address to the wireless client;

negotiating the establishment of a secure link with the wireless client using the assigned address; and

using the assigned address to communicate with clients via a wireless access point.

13. (Previously Presented) The method of claim 12, further comprising:

broadcasting an ARP packet to check whether there are any other clients having the same assigned address of the wireless client; and

if a response to the ARP packet is received, terminating the negotiation, thereby denying the wireless client access to the network.

14. (Previously Presented) The method of claim 12, further comprising:

in response to the negotiation, creating an ARP entry that maps the assigned address of the wireless client to a MAC address of the wireless client.

15. (Original) The method of claim 12, wherein the request is a DHCP discover packet, the method further comprising: inserting data into an optional field of the packet to indicate that the packet was received from a wireless client; and relaying the packet to the address server.

16. (Previously Presented) The method of claim 12, further comprising:

receiving a renewal request packet having a request for a renewal of the lease time from the wireless client;

if the secure link is successfully negotiated with the wireless client, inserting data into an optional field of the renewal request packet to indicate that the renewal request packet was received from a wireless client; and

relaying the renewal request packet to the address server.

17. (Original) A computer-readable medium having stored thereon computer-executable instructions for performing the method of claim 9.

18. (Original) A computer-readable medium having stored thereon computer-executable instructions for performing the method of claim 10.

19. (Original) A computer-readable medium having stored thereon computer-executable instructions for performing the method of claim 12.

20. (Original) A computer-readable medium having stored thereon computer-executable instructions for performing the method of claim 13.

21. (Original) On a wireless client, a method for gaining access to a network, the method comprising:

broadcasting a request for an address on the network;

receiving an assignment of a leased address from the network, the leased address having a lease time; and

negotiating a secure link with the network before the lease time expires.

22. (Original) The method of claim 21, wherein the request for an address is broadcast as a DHCP discover packet.

23. (Original) The method of claim 21, wherein the secure link is an IPSEC tunnel.

24. (Previously Presented) The method of claim 21, wherein the negotiating step further comprises:

generating an ARP packet having the lease address; and

in response to the ARP generation, initiating a negotiation of the secure link with the network.

25. (Original) The method of claim 21, wherein the leased address is received in a packet, wherein the packet additionally contains the network and MAC address of a wireless access point, wherein the secure link is negotiated with the wireless access point corresponding to the network address.

26. (Original) A computer-readable medium having stored thereon computer-executable instructions for performing the method of claim 21.

27. (Original) A computer-readable medium having stored thereon computer-executable instructions for performing the method of claim 22.

28. (Original) A computer-readable medium having stored thereon computer-executable instructions for performing the method of claim 23.

29. (Original) A computer-readable medium having stored thereon computer-executable instructions for performing the method of claim 24.

30. (Original) A computer-readable medium having stored thereon computer-executable instructions for performing the method of claim 25.

31. (Previously Presented) The method according to claim 1 wherein the assigned network address having the lease period is sent to the wireless client prior to authentication of the wireless client.

32. (Previously Presented) The method according to claim 1 wherein the lease period is of a duration that is sufficient for the wireless client to establish a secure link with the wireless access point and send a renewal request of the assigned address via the secure link.

33. (Previously Presented) The method according to claim 1 further comprising the step of extending the lease period of the assigned network address to a predefined duration if the wireless client establishes a secure link with the wireless access point and requests a renewal of the assigned address via the secure link.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None